Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US05/006015

International filing date: 24 February 2005 (24.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/549,356
Filing date: 02 March 2004 (02.03.2004)

Date of receipt at the International Bureau: 07 April 2005 (07.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

1301298

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 25, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/549,356*
FILING DATE: *March 02, 2004*
RELATED PCT APPLICATION NUMBER: *PCT/US05/06015*

Certified by

Jon W. Dudas

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

PTO/SB/16 (01-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. EV 406600026

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Harry	VIG	Billerica, MA

Additional inventors are being named on the _____ *separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☒ Customer Number: 36522

OR

☐ Firm or Individual Name					
Address					
Address					
City		State		Zip	
Country		Telephone		Fax	

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* 15 ☐ CD(s), Number _____

☒ Drawing(s) *Number of Sheets* 3 ☐ Other (specify) _____

☐ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☒ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fees.

☒ The Director is herby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 502992

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE Amount ($): $80-

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE Joseph E. Gortych

TYPED or PRINTED NAME Joseph E. Gortych

TELEPHONE 802-655-7222

Date March 2, 2004

REGISTRATION NO. 41,791 *(if appropriate)*

Docket Number: 022A-03P

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

4

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 80-

Complete if Known	
Application Number	
Filing Date	March 2, 2004
First Named Inventor	YIG, Harry
Examiner Name	N/A
Art Unit	N/A
Attorney Docket No.	022A-03P

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 502992

Deposit Account Name: MagiQ Technologies, Inc

The Director is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	80

SUBTOTAL (1) ($) 80-

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below	Fee Paid
Total Claims		-20** =		X =
Independent Claims		- 3** =		X =
Multiple Dependent				=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) N/A

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0

SUBMITTED BY				(Complete *(if applicable)*)	
Name *(Print/Type)*	Joseph E. Gortych	Registration No. *(Attorney/Agent)*	41,791	Telephone	8026557222
Signature	Joseph E. Gortych			Date	March 2, 2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

MODULATOR TIMING FOR QKD

Field of the Invention

The present invention relates to quantum cryptography, an in particular relates to a method for establishing the timing of the operation of modulators in a quantum key exchange (QKD) system.

Background of the Invention

Quantum key distribution involves establishing a key between a sender ("Alice") and a receiver ("Bob") by using weak (e.g., 0.1 photon on average) optical signals transmitted over a "quantum channel." The security of the key distribution is based on the quantum mechanical principal that any measurement of a quantum system in unknown state will modify its state. As a consequence, an eavesdropper ("Eve") that attempts to intercept or otherwise measure the quantum signal will introduce errors into the transmitted signals, thereby revealing her presence.

The general principles of quantum cryptography were first set forth by Bennett and Brassard in their article "Quantum Cryptography: Public key distribution and coin tossing," Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179 (IEEE, New York, 1984). Specific QKD systems are described in publications by C.H. Bennett et al entitled "Experimental Quantum Cryptography" and by C.H. Bennett entitled "Quantum Cryptography Using Any Two Non-Orthogonal States", Phys. Rev. Lett. 68 2121 (1992).

The general process for performing QKD is described in the book by Bouwmeester et al., "The Physics of Quantum Information," Springer-Verlag 2001, in Section 2.3, pages 27-33. During the QKD process, Alice uses a random number generator (RNG) to generate a random bit for the basis ("basis bit") and a random bit for the key ("key bit") to create a qubit (e.g., using polarization or phase encoding) and sends this qubit to Bob.

The above mentioned publications by Bennet each describe a so-called "one-way" QKD system wherein Alice randomly encodes the polarization or phase of single photons at one end of the system, and Bob randomly measures the polarization or phase of the photons at the other end of the system. The one-way system described in the Bennett 1992 paper is based on two optical fiber Mach-Zehnder interferometers. Respective parts of the interferometric system are accessible by Alice and Bob so that each can control the phase of the interferometer. The interferometers need to be actively stabilized to within a portion of quantum signal wavelength during transmission to compensate for thermal drifts.

U.S. Patent No. 6,438,234 to Gisin (the '234 patent), which patent is incorporated herein by reference, discloses a so-called "two-way" QKD system that is autocompensated for polarization and thermal variations. Thus, the two-way QKD system of the '234 patent is less susceptible to environmental effects than a one-way system.

However, QKD systems such as '234 are typically described as operating in their ideal operating state without any description of how the ideal state is reached. As it turns out, setting up a QKD system to operate in an ideal state is a daunting task since QKD system operation involves exchanging weak pulses that need to be modulated at very precise times.

Summary of the Invention

A first aspect of the invention is a method of setting up the timing for the phase modulators in a two-way QKD system. The method includes selecting an initial time T0, an initial modulation voltage V_B (e.g., $V_B[\pi]$) and a relatively large initial voltage signal width WB for Bob's modulator MB. The method also includes sending delayed pulses P1 and P2 from Bob to Alice and receiving the pulses back at Bob without any modulation at Alice's modulator MA. The method further includes counting the pulses that are to be modulated by Bob at Bob's detectors. If no modulation by Bob's modulator occurs, then the method includes iteratively incrementing the voltage timing by a coarse time interval and

observing whether the detectors indicate that modulation has occurred. When modulation occurs, as indicated by a shift in the counts between the detectors, then the voltage timing is reset to a time T1 that yields the change in detector counts. The coarse time interval is then sub-divided into fine time intervals. The voltage signal width is reduced and the timing is adjusted from T1 by increments of the fine time interval to further narrow down the precise voltage timing. This process of iteratively resetting the timing, subdividing the previous time intervals and then incrementing the timing by the new sub-interval is repeated until the modulator voltage timing is deduced to a desired degree of accuracy. The voltage timing may ultimately be adjusted along the way to center the voltage signal to the arrival of the pulse to be modulated.

Once Bob's timing T_{VB} is established, then Bob's modulator voltage is fixed at V_B ($V_B[\pi]$) and Alice's modulator voltage V_A is set to $V_A = -V_B = V_A[-\pi]$. Also, the modulator voltage width WA is set to be relatively large and a (new) initial voltage signal (leading edge) timing T0 is selected. The iterative process described above for Bob is repeated essentially the same for Alice with respect to the coarse and fine adjustment of the timing and adjusting the voltage signal width WA to establish a final timing T_{VA} that is centered about the pulse that is modulated by Alice.

In an example embodiment, one of the pulses is modulated both as it enters and as it leaves Alice. This allows for Alice's modulator to modulate the pulse for orthogonal polarizations. Since phase modulators tend to be polarization sensitive, this approach serves to reduce modulation error that results from polarization variations in the pulses.

Brief Description of the Drawings

FIG. 1 is a schematic diagram of a two-way QKD system;

FIG. 2 is a flow diagram of an example embodiment of the method of establishing the modulator timing in the two-way QKD system of FIG. 1 for Bob's modulator; and

FIG. 3 is a flow diagram of an example embodiment of the method of establishing the modulator timing in the two-way QKD system of FIG. 1 for Alice's modulator.

Detailed Description of the Invention

The present invention relates to quantum cryptography, and in particular relates to systems and methods for performing phase or polarization modulation in quantum key exchange (QKD) system. The ideal operation of a two-way QKD system is described immediately below, followed by descriptions of example embodiments of the timing set-up.

Two-way QKD system

FIG. 1 is a schematic diagram of a two-way QKD system 100. Bob includes laser 12 that emits light pulses P0. Laser 12 is coupled to a time-multiplexing/demultiplexing (M/D) optical system 104. M/D optical system 104 receives input pulses P0 from laser 12 and splits each pulse into two time-multiplexed pulses P1 and P2. Likewise, optical system 104 receives from Alice (discussed below) pairs of time-multiplexed pulses and combines (interferes) them into a single pulse. Bob also includes a phase modulator MB coupled to an M/D optical system on the side opposite laser 12. Optical fiber link FL is coupled to phase modulator MB and connects Bob to Alice. Bob also includes a voltage controller 44 coupled to modulator MB, and a random number generator (RNG) unit 46 coupled to the voltage controller.

Bob also includes two detectors 32a and 32b coupled to M/D optical system 104, and a controller 50 operatively (e.g., electrically) coupled to laser 12, detectors 32a and 32b, voltage controller 44 and to RNG unit 46.

Alice includes a phase modulator MA coupled at one end to optical fiber link FL and at the opposite end to a Faraday mirror FM. Alice also includes voltage controller 14 coupled to modulator MA, and random number generator (RNG) unit 6 coupled to the voltage controller. Alice further includes controller 20 coupled to RNG unit 16 and to voltage controller 14.

Bob's controller 50 is coupled (optically or electronically) to Alice's controller 20 via synchronization channel SL to synchronize the operation of Alice and Bob. In particular, the operation of the phase modulators MA and MB is coordinated by controllers 20 and 50 exchanging synchronization signals SS. In an example embodiment, the operation of the entire system, including the timing set-up of the present invention, is controlled from either controller 20 or controller 50.

Example operational embodiment of two-way QKD system

In an example embodiment of the operation of QKD system 100, Bob's controller 50 sends a signal S0 to laser 12, which in response thereto initiates a relatively strong, short laser pulse P0, which is then attenuated by an optional variable optical attenuator VOA 13B. The (weak) pulse P0 arrives at M/D optical system 104, which splits the pulse into two weak pulses, P1 and P2, having orthogonal polarization. Pulse P1 goes directly towards Alice while P2 is delayed. Pulses P1 and P2 pass through MB (which remains inactivated at this point), and the pulses travel down the fiber to Alice.

Note that in another embodiment of system 100, pulses P0 and P1 can be relatively strong pulses that are attenuated by Alice using a VOA 13A located at Alice, wherein the pulses are attenuated to make them weak (quantum) pulses prior to them returning to Bob.

The pulses pass through Alice's modulator MA and reflect off of Faraday mirror FM, which changes the polarization of the pulses by 90°. As the pulses travel back through modulator MA, Alice lets the first pulse P1 pass therethrough unmodulated but modulates the phase (i.e., imparts a phase shift Φ_A to) second pulse P2.

The timing of the modulation is provided by the synchronization signal SS shared between controllers 20 and 50, as described in greater detail below. The modulation at Alice is carried out by controller 20 providing a well-timed signal S1 to RNG unit 16, which provides a signal S2 representative of a random number to voltage controller 14. In response, voltage controller 14 sends a voltage signal

V_A (e.g., V[+3π/4], [V-3π/4], V[+π/4], and V[-π /4]) to modulator MA to set the phase modulation to a corresponding value +3π/4, -3π/4, π/4 or -π /4.

The two pulses P1 and P2 then travel back to Bob, where, say, pulse P2 passes unaltered through modulator MB, but where Bob imparts a phase shift Φ_B to pulse P1. The timing of the modulation of pulse P1 (or any other selected pulse) at Bob is provided by the synchronization signal SS shared between controllers 20 and 50, as described in greater detail below. The modulation is carried out by controller 50 providing a well-timed signal S3 to RNG unit 46, which provide a signal S4 representative of a random number to voltage controller 44. In response, voltage controller 44 sends a voltage signal V_B (e.g., V[+π/4] or V[-π/4]) to modulator MB to set the phase modulation to a corresponding value +π/4 or -π /4.

Further, when pulses P1 and P2 enter M/D optical system 104, pulse P2 passes directly through but pulse P1 is delayed by an equal amount equal to that originally imparted to pulse P2. M/D optical system then interferes pulses P1 and P2.

The detectors 32a and 32b are arranged so that constructive interference ($\Phi_A - \Phi_B = 0$) is detected by detector 32a and destructive interference ($\Phi_A - \Phi_B = \pi$) is detected by detector 32b. When Bob imparts the same basis phase as Alice, a count in detector 32a indicates binary 0 and a count in detector 32b indicates binary 1. However, when Bob's basis phase is different from Alice's, there is no correlation and the count winds up in either detector 32a or 32b with equal probability (i.e., interfered the pulse has a 50:50 chance of being detected in either detector).

Modulator timing set-up

The description above relates to an idealized QKD system. However, in practice, such systems do not automatically operate in the ideal state. Further, a commercially realizable system must first be set up to operate and then must be able to compensate for changes in its operating state to ensure ongoing operation.

Accordingly, prior to running a QKD system in the idealized manner described above, the system must first be calibrated. This includes calibrating the phase modulators so that the proper phase encoding is achieved.

In order to even calibrate the modulators in a QKD system, the proper timing of the activation of the modulators must first be established. Specifically, each modulator must be activated at the precise moment the pulse that needs to be modulated passes through the particular modulator. Minimizing the amount of time a modulator is activated reduces the chances of an eavesdropper determining the modulator state in an attempt to gain information about the exchanged key.

Thus, an example embodiment of the present invention includes setting up the modulator timing. For each modulator, the method includes two main steps: a coarse timing adjustment with a wide modulation voltage signal W followed by a fine timing adjustment with a narrow modulation voltage signal width W.

These basic steps are now described in greater detail below with reference to QKD system 100 of FIG. 2. Note that in an example embodiment, controllers 20 and 50 communicate directly with their respective voltage controllers 14 and 44 via respective calibration signals SC1 and SC2 in the modulator timing set-up rather than through RNG units 16 and 46.

Timing for Bob's modulator

In an example embodiment, the timing for Bob's modulator MB is established, though Alice's timing could be established first.

With reference to flow diagram 200 of FIG. 2, in 202, Bob's controller 50 sends a signal SS over synchronization channel SL to controller 20 instructing it to turn off Alice's phase modulator if it is not already off. In 204, controller 50 then directs voltage controller 44 to set the modulator voltage V_B to a relatively large modulation value, such as $V_B[\pi]$. The voltage setting of $V_B[\pi]$ is preferable because it allows for fewer photons (e.g., hundreds) per pulse to be used as compared to other voltage settings that require more (i.e., thousands) of photons per pulse. This translates into a faster scan time and thus faster timing set-up

operation. Thus, even though the particular bases used in the key exchange operation might not include a phase setting of π, for the purposes of setting up the modulator timing as quick as possible, this phase setting may be preferred.

In 206, controller 50 also directs voltage controller 44 to make the width WB of voltage signal $V_B[\pi]$ relatively large (say, 50ns) as compared to the final voltage signal width (which is typically in the range from 2ns to 10ns). In 208, controller 50 selects an initial modulator voltage time T0 at which $V_B[\pi]$ is to be applied to modulator MB. In an example embodiment, T0 = 0.

In 210, controller 50 then sends a signal S0 to laser 12 to generate pulses P0 at a given repetition rate, such as 1MHz. Pulses P0 need not be quantum pulses and can have hundreds or thousands of photons. In an example embodiment, the average number of photons μ in pulses P0 is selected to be that necessary to readily discern the detection of photons in detectors 32a and 32b. In such a case, μ is typically between 1 and 10.

In 212, modulator MB is modulated with $V_B[\pi]$ at T0 and with width WB, and the photon count at detectors 32a and 32b is measured. If the timing of modulator MB is not correct, then no pulses will be modulated and the photon count at detector 32a will be high, while the photon count at detector 32b will be low and originating mostly from dark current and other spurious effects.

Note that in system 100 of FIG. 1, two pulses P1 and P2 are created from pulse P0. These pulses are reflected from Alice and return to Bob. In system 100 as described above, the relative phase difference between P1 and P2 at the end of a round trip along optical fiber link FL is measured by detectors 32a and 32b.

In system 100, the phase modulation from modulators MA and MB can be imparted to P1 by both Alice and Bob, imparted to P2 by both Alice and Bob, imparted to P1 by Bob and to P2 by Alice or vice versa, since it is the overall relative phase difference between the pulses that is ultimately measured, not the phase of any particular pulse. However, the particular phase modulation method must be agreed upon in advance by Alice and Bob so as to set the modulator voltage amplitudes and the voltage pulse timing to the correct levels.

In the example embodiment described below, it is presumed that, pulse P1 is modulated by both Alice and by Bob for the sake of illustration. The phase shift is the sum given by each modulator, and is compared to the phase of the unmodulated pulse P2. Thus, in an example embodiment of the modulator timing set-up, it is the modulation of pulse P1 through Alice that needs to be timed, If both pulses P1 and P2 are to be modulated, the timing set-up method of the present invention applies to this case in a straightforward manner. For example, , if P1 is modulated by Bob and P2 is modulated by Alice, then a bias phase voltage of $V_B = V_A = V[\pi]$ needs to be provided to both modulators to ensure a null phase difference.

It is important that Bob's outgoing pulses P1 and P2 not be modulated because this could reveal information of Bob's modulator state .to an eavesdropper. This is particularly true when a high average photon level μ is used, since is allows an eavesdropper to place a tap on the fiber link FL without detection.

After a sufficient sampling interval, resulting in say at least 10 photons or more in the presence of external noise, the photon count of each detector is recorded, and in 214 the pulse timing T0 (measured, say, at the leading edge of the voltage signal) is incremented by ΔT. The value of ΔT is selected to be slightly smaller than initially wide modulator pulse. For example, for a 1MHz repetition rate from laser 12, the pulses P0 are separated by 1μs. This interval can be divided, say, into 25 segments, to define a (coarse) time increment ΔT = 40ns which can be covered with a 50ns modulator pulse width to guarantee overlap.

Also in 214, the photon count is checked again to see if modulation has occurred. If not, then T0 is incremented by another ΔT, etc., 212 is repeated and and the photon count check of 214 is repeated. Acts 212 and 214 are repeated (iterated) n times for $T0 + n\Delta T$ until the entire interval between successive laser pulses is covered. Note that by setting $V_B = V_B[\pi]$, the shift in photon count is dramatic when the phase modulation finally occurs, as compared to setting V_B to $V_B[\pi/4]$, as is the case for normal QKD system operation.

This process results in two time intervals during which photons are detected on detector 32b rather than detector 32a. One such time interval occurs when photons from laser 12 are affected by the modulator MB during travel towards Alice, and one interval when the photons returning from Alice travel through the modulator MB. If the length of the fiber link FL was changed so that the round trip travel time was increased, then the outgoing pulse would show a photon deflection event at the same point in time, while the return pulse would result in a photon deflection event at a time corresponding to the delay due to the increase in round-trip travel time.

A similar effect can be achieved without changing the physical fiber by changing the rate at which photon pulses P0 are sent in to the system. Since there is more than one pulse in the fiber link FL, this will cause an apparent change in location of the return pulse. Thus, in 215, the modulator MB is set to the timing (say, T1) that only modulates pulses incoming to Bob, which corresponds to the pulses that change locations.

Once the shift in the photon counts occurs between the detectors so that the outgoing pulse timing T1 for Bob can be identified, then the process proceeds to 216, wherein the timing is set to T1. However, the modulation timing at this point is only known to within the timing increment ΔT, which in our example is 50ns.

The modulation voltage width WB of the voltage signal V_B needs to be decreased to a more reasonable value. Ideally, voltage signal V_B ultimately has a width WB that is as small as possible so that modulator MB is activated only for the briefest amount of time necessary to modulate incoming pulse P1. Also, the voltage signal width WB needs to be small enough so that incoming pulse P2, which is close to incoming pulse P1 (e.g., within a few nanoseconds), passes through modulator MB without being modulated.

Accordingly, in 217 the width WB is reduced, e.g., to 5ns. This value is picked with physical bandwidth and settling time limitations of the modulator voltage driver 14 in mind. Thus, in 218 the increment ΔT is broken divided into a number of (fine) sub-intervals, say $\Delta T' = (50ns)/(25) = 2ns$, which should be

smaller than width WB to allow overlap during scanning. In 218, acts 214-216 are then repeated using T2 = T1 + $n\Delta T'$ until the value of T2 is determined to within $\Delta T'$ (here, $\Delta T'$ = 2ns). The timing pulse is then centered about the intervals at which the photon counts at the detectors show changes.

In 224 and 226, the process of finding the modulation voltage timing T1 and T2, (optionally) narrowing voltage signal width WB and subdividing the time increment into increasingly smaller segments in 212-218 is optionally repeated for additional voltage timing values T3, T4, etc. using correspondingly smaller time sub-intervals and optionally smaller voltage signal widths WB until the final timing T_{VB} of the modulator voltage V_B for modulator MB is established to a desired degree of accuracy, e.g.,t0 2ns or so, with a final pulse width WB of about 2ns.

Timing for Alice's modulator

Once the timing of Bob's modulator MB is established, then the timing of Alice's modulation is established. Note that in another example embodiment, Alice's modulator timing can be established first.

Accordingly, with continuing reference to FIG. 1 and also to the flow diagram 300 of FIG. 3B, in 302 Bob's modulator voltage is set constant at $V_B[\pi]$.

In 304, Alice's controller 20 sends a signal SC2 to voltage controller 14 directing it to send a voltage signal $V_A = -V_B = V_A[-\pi]$ to modulator MA. This serves to set the phase of modulator MA to (nominally) $-\pi$. Bob's modulator MB is maintained constant at $V_B[\pi]$ during Alice's modulator timing set-up. As with Bob's modulator voltage V_B, Alice's modulator voltage V_A is set to a relatively large modulation value, such as $V_A[-\pi]$ so that if modulation occurs, an overall phase shift of (nominally) 0 results, which results in the modulated pulses being detected at detector 32a. If no modulation occurs, then the pulses will have a phase of π, which results in the modulated pulses being detected at detector 32b.

In 306, as in 206 for Bob, controller 20 also directs voltage controller 44 to make the width WA of voltage signal $V_A[\pi]$ relatively large (say, 50ns) as compared to the final signal width (which is typically about 10ns).

In 308, as in 208 for Bob, controller 20 selects a (new) initial time T0 at which $V_A[-\pi]$ is to be applied to modulator MA.

Note that in an example embodiment, the optical pulse to be modulated at Alice is modulated both on the way in and on the way out of Alice. This requires width WA to be wide enough to modulate the pulse as it travels through the modulator to the Faraday mirror and back through the modulator, yet narrow enough not to modulate both pulses P1 and P2. This modulation approach has the advantage of reducing the polarization sensitivity of the modulator to variations in the pulse polarizations.

In 310, as in 210 for Bob, controller 50 then sends a signal S0 to laser 12 to generate pulses P0 at a given repetition rate, such as 1MHz.

In 312, as in 212 for Bob, the photon count at detectors 32a and 32b is measured. If the timing of modulator MA is incorrect, then pulse P2 passing through the modulator on the way back to Bob will not be modulated at Alice and the photon count at detector 32b will be high, while the photon count at detector 32a will be low and be due mostly to dark current and other spurious effects.

Recall that in system 100 of FIG. 1, two pulses P1 and P2 are created from pulse P0. These pulses are reflected from Alice and return to Bob. In system 100 as described above, either pulse P1 or pulse P2 is modulated by Alice and either pulse P1 or pulse P2 is modulated by Bob. Thus, in the modulator timing set-up for Alice, it is the modulation of previously agreed upon pulse P1 or P2 that needs to be timed, and it needs to be modulated on both the way into Alice and the way out of Alice.

Unlike the situation at Bob, the round trip time for a photon to travel from modulator MA, to the faraday mirror MF, and back to modulator MA is well known as does not change to any appreciable degree. This round trip travel time is smaller than the time separating P1 and P2. Modulator MA is driven with a sufficiently narrow modulator drive voltage width WA to observe two changes in

photon detector counts:, one corresponding to the transition in and out of P1, and the second corresponding to the transition out of P2. The modulator drive pulse VA has a width WA sufficient to cover both directions of travel of P1 or P2 at the same time.

If the photon count indicates no modulation has occurred, then in 314 the voltage signal timing T0 is incremented by ΔT, as in 214 for Bob. The value of ΔT is selected, for example, by knowing the time interval between pulses P1 and P2 so as to guarantee that only one pulse is modulated at a time. In 214, the photon count is checked again to see if modulation has occurred. If not, then T0 is incremented by another ΔT, etc., and photon count check is repeated. This process is repeated n times for $T0 + n\Delta T$ until the entire interval between successive laser pulses is covered.

Recall, at Bob only one direction of travel of pulses P1 or P2 is covered by the modulator voltage signal V_B. However, in Alice, both directions of travel of the pulses is covered by the modulator voltage signal VA. Thus, in the case of Bob, a change in photon count of say, less around 50%, would not be wholly indicative of a change in the modulation. On the other hand, such a change at Alice could very well indicate that at least one of the two modulations of the pulse to be modulated has occurred and that at least a rough estimate of the timing has been established.

In a fashion similar to that carried out for Bob, this timing-shift process is repeated with finer accuracy. Once a shift in photon counts between the detectors occurs, then the process proceeds to 316, wherein the timing T1 is set to the beginning of the interval of the photon count change, and acts 312 and 314 are repeated (iterated) with sub-intervals $\Delta T'$, as discussed above in 216 for Bob, until the value of T2 is determined (e.g., to within $\Delta T' = 2ns$). At this point, the photon count of detector 32b will be near zero again, as both direction of travel for either photon pulse P1 or P2 are covered.

Once the timing for voltage signal $V_A[-\pi]$ is established, then as in 217 of Bob, in 317 the width WA of the voltage signal $V_A[-\pi]$ is decreased to a smaller value to make probing modulator MA by an eavesdropper more difficult. In an

example embodiment the voltage signal width WA is made incrementally smaller and acts 312-316 repeated with the smaller signal width.

Then, as in 218 of Bob, in 318 the timing interval ΔT is divided into finer sub-intervals $\Delta T'$ and acts 312-316 are repeated. If a change occurs in the photon count that indicates a change back to the "no modulation" state, then in 322, as in 222 for Bob, the modulator voltage timing T_{VA} is adjusted to shift the narrowed voltage signal until modulation is reestablished, and preferably so the narrowed voltage signal is centered on the pulse P2. In 324, acts 317 and 320 (or 318-320) are then repeated until the desired width Alice modulator voltage timing T_{VA} is established. In an example embodiment, the voltage signal width WA is about 5X the width of voltage signal width WB, e.g., WB = 2ns and WA = 10ns.

In an example embodiment, the modulator timing set-up is accomplished by including software in controllers 20 and 50 that has instructions for carrying out the timing method discussed above and illustrated in the corresponding flow diagrams.

Not also that the modulator timing set-up process must be repeated if the fiber length is changed, (e.g., a connection to a new fiber link FL or optical switching to a new optical path), or if the qbit update rate changes.

While the present invention has been described in connection with preferred embodiments, it will be understood that it is not so limited. On the contrary, it is intended to cover all alternatives, modifications and equivalents as may be included within the spirit and scope of the invention as defined in the appended claims.

ABSTRACT

Methods for establishing modulator timing for a two-way QKD system having QKD stations Bob and Alice are disclosed. The timing method includes performing a coarse timing adjustment by scanning the modulator timing domain with a relatively coarse timing interval and wide modulator voltage signal, and then performing a fine timing adjustment by scanning the modulator timing domain with a fine timing interval and a relatively narrow modulator voltage signal. The timing method includes monitoring the detector counts to determine when modulation is occurring and setting the timing accordingly. The method further includes discerning between two timing intervals associated with pulses entering and leaving Bob, and ensuring that only incoming pulses are modulated.

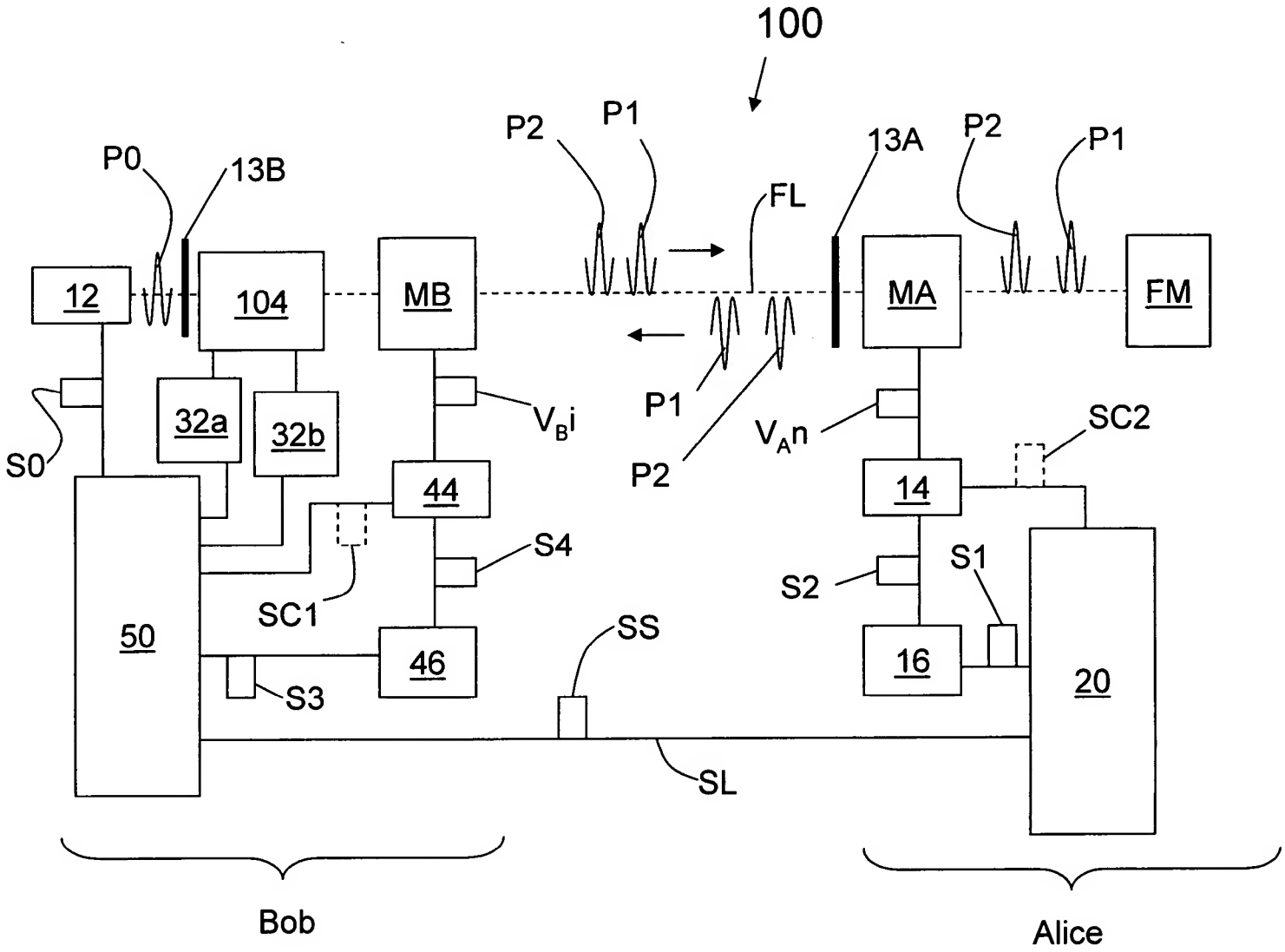
100
P0
13B
P2
P1
FL
13A
P2
P1
12
104
MB
MA
FM
P1
P2
V_Bi
V_An
S0
32a
32b
44
14
SC2
S4
S1
S2
SC1
50
SS
46
16
20
S3
SL
Bob
Alice

FIG. 1

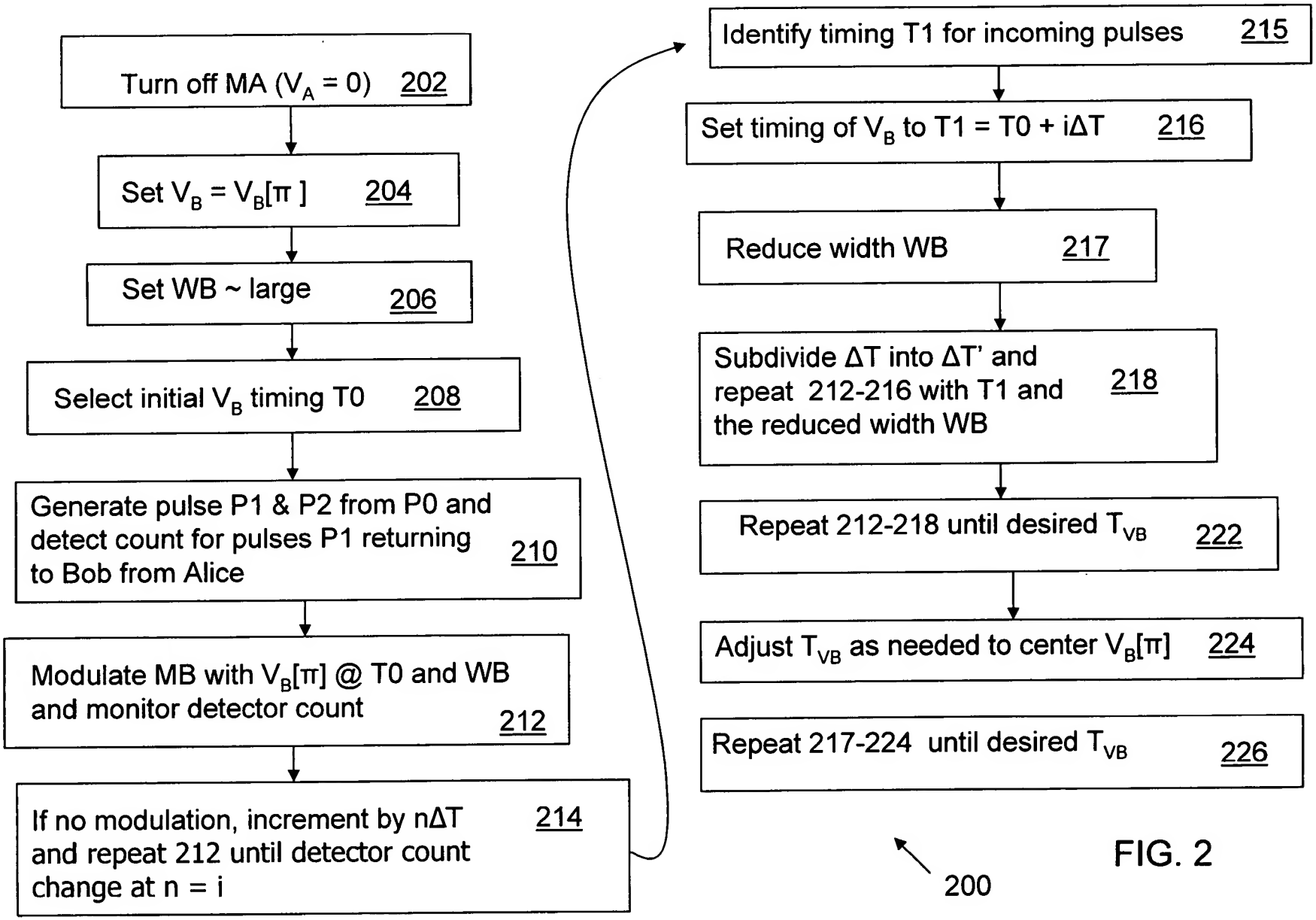
Turn off MA (V_A = 0) 202
Set V_B = $V_B[\pi]$ 204
Set WB ~ large 206
Select initial V_B timing T0 208
Generate pulse P1 & P2 from P0 and detect count for pulses P1 returning to Bob from Alice 210
Modulate MB with $V_B[\pi]$ @ T0 and WB and monitor detector count 212
If no modulation, increment by nΔT and repeat 212 until detector count change at n = i 214
Identify timing T1 for incoming pulses 215
Set timing of V_B to T1 = T0 + iΔT 216
Reduce width WB 217
Subdivide ΔT into ΔT' and repeat 212-216 with T1 and the reduced width WB 218
Repeat 212-218 until desired T_{VB} 222
Adjust T_{VB} as needed to center $V_B[\pi]$ 224
Repeat 217-224 until desired T_{VB} 226
200

FIG. 2

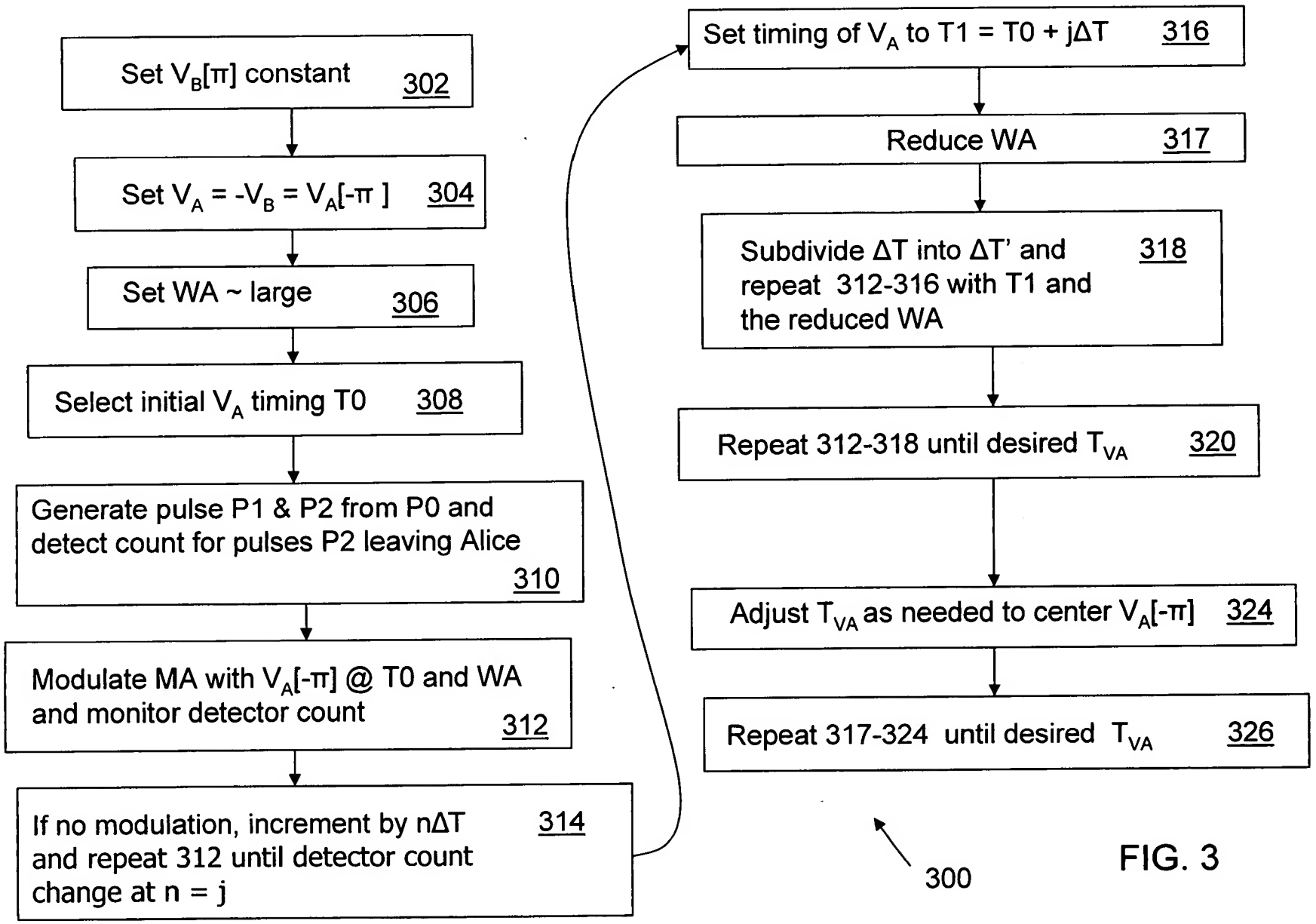
Set $V_B[\pi]$ constant 302
Set $V_A = -V_B = V_A[-\pi]$ 304
Set WA ~ large 306
Select initial V_A timing T0 308
Generate pulse P1 & P2 from P0 and detect count for pulses P2 leaving Alice 310
Modulate MA with $V_A[-\pi]$ @ T0 and WA and monitor detector count 312
If no modulation, increment by nΔT and repeat 312 until detector count change at n = j 314
Set timing of V_A to T1 = T0 + jΔT 316
Reduce WA 317
Subdivide ΔT into ΔT' and repeat 312-316 with T1 and the reduced WA 318
Repeat 312-318 until desired T_{VA} 320
Adjust T_{VA} as needed to center $V_A[-\pi]$ 324
Repeat 317-324 until desired T_{VA} 326
300

FIG. 3